Context-gebaseerde toegangscontrole (CBAC) configureren

Inhoud

Inleiding

De Context-Based Access Control (CBAC) optie van de Cisco IOS Firewallfunctieset inspecteert actief de activiteit achter een firewall. CBAC specificeert welk verkeer moet worden ingehuurd en welk verkeer eruit moet worden gehaald door gebruik te maken van toegangslijsten (op de dezelfde manier dat Cisco IOS toegangslijsten gebruikt). In de toegangslijsten van CBAC worden echter ook IP-inspecties opgenomen, zodat het protocol kan worden geïnspecteerd om er zeker van te zijn dat er niet met wordt geknoeid voordat het protocol naar de systemen achter de firewall gaat.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Achtergrondinformatie

CBAC kan ook worden gebruikt bij Network Address Translation (NAT), maar de configuratie in dit document heeft voornamelijk betrekking op pure inspectie. Als u NAT uitvoert moeten uw toegangslijsten de globale adressen weerspiegelen, niet de echte adressen.

Denk aan deze vragen voor de configuratie.

- Welk verkeer wil je vrijlaten?
- Welk verkeer wil je binnenlaten?
- Welk verkeer wil je inspecteren?

Welk verkeer wil je weglaten?

Welk verkeer je wilt uitzetten is afhankelijk van je beveiligingsbeleid, maar in dit algemene voorbeeld is alles uitgaande toegestaan. Als je toegangslijst alles ontkent, dan kan er geen verkeer vertrekken. Specificeer uitgaande verkeer met deze uitgebreide toegangslijst:

```
access-list 101 permit ip [source-network] [source-mask] any
access-list 101 deny ip any any
```

Welk verkeer wil je binnenlaten?

Welk verkeer u wilt laten, is afhankelijk van uw beveiligingsbeleid. Maar het logische antwoord is alles wat uw netwerk niet beschadigt.

In dit voorbeeld is er een lijst van verkeer die logisch lijkt in te lassen. Het verkeer van Internet Control Message Protocol (ICMP) is over het algemeen aanvaardbaar, maar het kan bepaalde mogelijkheden voor DOS-aanvallen toestaan. Dit is een voorbeeldtoegangslijst voor inkomend verkeer:

Uitgebreide IP-toegangslijst 101

```
permit tcp 10.10.10.0 0.0.0.255 any (84 matches)
permit udp 10.10.10.0 0.0.0.255 any
permit icmp 10.10.10.0 0.0.0.255 any (3 matches)
deny ip any any
```

Uitgebreide IP-toegangslijst 102

```
permit eigrp any any (486 matches)
permit icmp any 10.10.10.0 0.0.0.255 echo-reply (1 match)
permit icmp any 10.10.10.0 0.0.0.255 unreachable
permit icmp any 10.10.10.0 0.0.0.255 administratively-prohibited
permit icmp any 10.10.10.0 0.0.0.255 packet-too-big
permit icmp any 10.10.10.0 0.0.0.255 echo (1 match)
permit icmp any 10.10.10.0 0.0.0.255 time-exceeded
deny ip any any (62 matches)

access-list 101 permit tcp 10.10.10.0 0.0.0.255 any
access-list 101 permit udp 10.10.10.0 0.0.0.255 any
```

```
access-list 101 permit icmp 10.10.10.0 0.0.0.255 any
access-list 101 deny ip any any

access-list 102 permit eigrp any any
access-list 102 permit icmp any 10.10.10.0 0.0.0.255 echo-reply
access-list 102 permit icmp any 10.10.10.0 0.0.0.255 unreachable
access-list 102 permit icmp any 10.10.10.0 0.0.0.255 administratively-prohibited
access-list 102 permit icmp any 10.10.10.0 0.0.0.255 packet-too-big
access-list 102 permit icmp any 10.10.10.0 0.0.0.255 echo
access-list 102 permit icmp any 10.10.10.0 0.0.0.255 time-exceeded
access-list 102 deny ip any any
```

Toegangslijst 101 is voor het uitgaande verkeer. Toegangslijst 102 is voor het inkomende verkeer. De toegangslijsten staan slechts een Routing Protocol, Enhanced Interior Gateway Routing Protocol (DHCP) en een gespecificeerd ICMP-inkomende verkeer toe.

In het voorbeeld is een server aan de Ethernet kant van de router niet toegankelijk van het internet. De toegangslijst weerhoudt het van het opzetten van een sessie. Om het toegankelijk te maken, moet de toegangslijst worden gewijzigd om het gesprek mogelijk te maken. Als u een toegangslijst wilt wijzigen, verwijdert u de toegangslijst, bewerkt u de lijst en past u de bijgewerkte toegangslijst opnieuw toe.

Opmerking: de reden dat u de toegangslijst 102 verwijdert voordat u deze bewerkt en opnieuw toepast, is te wijten aan "elke willekeurige toegangslijst weigeren" aan het einde van de toegangslijst. In dit geval, als u een nieuwe ingang zou toevoegen alvorens u de toegang-lijst verwijdert, verschijnt de nieuwe ingang na ontkennen. Daarom wordt het nooit gecontroleerd.

Dit voorbeeld voegt het Simple Mail Transfer Protocol (MTP) toe slechts voor 10.10.10.1.

Uitgebreide IP-toegangslijst 102

```
permit eigrp any any (385 matches)
permit icmp any 10.10.10.0 0.0.0.255 echo-reply
permit icmp any 10.10.10.0 0.0.0.255 unreachable
permit icmp any 10.10.10.0 0.0.0.255 administratively-prohibited
permit icmp any 10.10.10.0 0.0.0.255 packet-too-big
permit icmp any 10.10.10.0 0.0.0.255 echo
permit icmp any 10.10.10.0 0.0.0.255 time-exceeded
permit tcp any host 10.10.10.1 eq smtp (142 matches)
!--- In this example, you inspect traffic that has been !--- initiated from the inside network.
```

Welk verkeer wil je controleren?

CBAC binnen Cisco IOS ondersteunt:

Naam van het sleutelwoord	Protocol
praatje	UCSeMe-protocol
ftp	File Transfer Protocol
h323	H.323-protocol (bijvoorbeeld Microsoft NetMeeting of Intel Video Phone)
http	HTTP-protocol
rcmd	R-opdrachten (r-exec, r-login, r-sh)
realaudio	Real Audio-protocol

rpc	Remote-gespreksprotocol
beuken	Eenvoudig mailoverdrachtprotocol
sqlnet	SQL NetProtocol
stroomlijnen	StreamWorks-protocol
tcp	Transmissiebeheerprotocol
tftp	TFTP-protocol
udp	User Datagram Protocol
levend	VDOLive-protocol

Elk protocol is gebonden aan een sleutelnaam. Pas de sleutelwoordnaam op een interface toe die u wilt inspecteren. Bijvoorbeeld, deze configuratie inspecteert FTP, MTP, en Telnet:

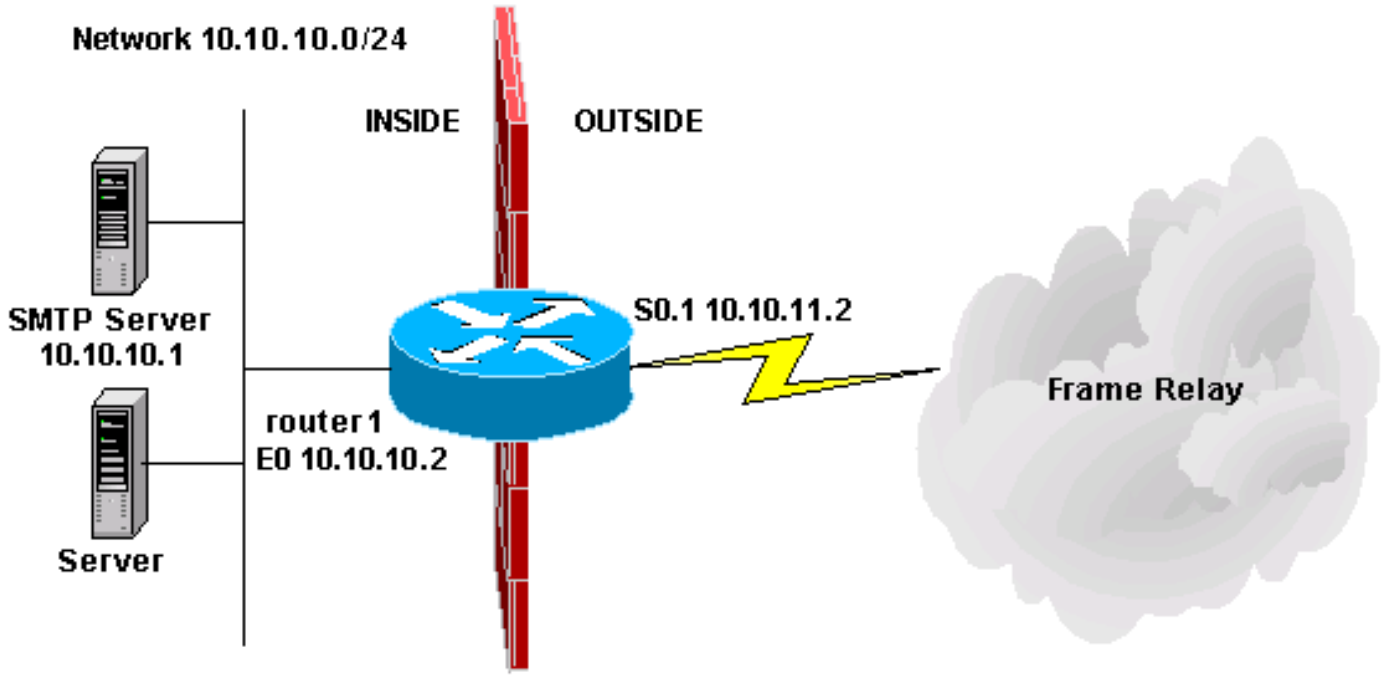
```
router1#configure
Configuring from terminal, memory, or network [terminal]? Enter configuration
commands, one per line. End with CNTL/Z.
router1(config)#ip inspect name mysite ftp
router1(config)#ip inspect name mysite smtp
router1(config)#ip inspect name mysite tcp
router1#show ip inspect config
Session audit trail is disabled
one-minute (sampling period) thresholds are [400:500]connections
max-incomplete sessions thresholds are [400:500]
max-incomplete tcp connections per host is 50.
Block-time 0 minute.
tcp synwait-time is 30 sec -- tcp finwait-time is 5 sec
tcp idle-time is 3600 sec -- udp idle-time is 30 sec
dns-timeout is 5 sec
Inspection Rule Configuration
Inspection name mysite

ftp timeout 3600
smtp timeout 3600
tcp timeout 3600
```

Dit document richt zich op wat u wilt weglaten, welk verkeer u wilt binnenlaten en welk verkeer u wilt inspecteren. Nu u klaar bent om CBAC te configureren voltooien u deze stappen:

1. Pas de configuratie toe.
2. Voer de toegangslijsten in zoals hierboven ingesteld.
3. Configureer de inspectieverklaringen.
4. Pas de toegangslijsten op de interfaces toe.

Na deze procedure verschijnt uw configuratie zoals in dit diagram en de configuratie wordt weergegeven.



Op context gebaseerde toegangscontrole-configuratie

```
!
version 11.2
no service password-encryption
service udp-small-servers
service tcp-small-servers
!
hostname router1
!
!
no ip domain-lookup
ip inspect name mysite ftp
ip inspect name mysite smtp
ip inspect name mysite tcp
!
interface Ethernet0
ip address 10.10.10.2 255.255.255.0
ip access-group 101 in
ip inspect mysite in


no keepalive
!
interface Serial0
no ip address
encapsulation frame-relay
no fair-queue
!
interface Serial0.1 point-to-point
ip address 10.10.11.2 255.255.255.252
ip access-group 102 in
frame-relay interface-dlci 200 IETF
!
router eigrp 69
network 10.0.0.0
no auto-summary
!
ip default-gateway 10.10.11.1
no ip classless
ip route 0.0.0.0 0.0.0.0 10.10.11.1
```

```
access-list 101 permit tcp 10.10.10.0 0.0.0.255 any
access-list 101 permit udp 10.10.10.0 0.0.0.255 any
access-list 101 permit icmp 10.10.10.0 0.0.0.255 any
access-list 101 deny ip any any
access-list 102 permit eigrp any any
access-list 102 permit icmp any 10.10.10.0 0.0.0.255
echo-reply
access-list 102 permit icmp any 10.10.10.0 0.0.0.255
unreachable
access-list 102 permit icmp any 10.10.10.0 0.0.0.255
administratively-prohibited
access-list 102 permit icmp any 10.10.10.0 0.0.0.255
packet-too-big
access-list 102 permit icmp any 10.10.10.0 0.0.0.255
echo
access-list 102 permit icmp any 10.10.10.0 0.0.0.255
time-exceeded
access-list 102 permit tcp any host 10.10.10.1 eq smtp
access-list 102 deny ip any any
!
line con 0
line vty 0 4
login
!
end
```

Gerelateerde informatie

- Cisco IOS-ondersteuningspagina voor firewall
- Technische ondersteuning en documentatie – Cisco Systems